Identity Theft: Do Definitions Still Matter?

Julia S. Cheney*

August 2005

Summary: *Despite a statutory definition of identity theft, there is a continuing debate on whether differences among the financial frauds associated with identity theft warrant further distinction and treatment, not only by lenders and financial institutions but also by consumers and regulatory and law enforcement agencies. In this Discussion Paper, Julia S. Cheney examines four types of financial fraud – fictitious identity fraud, payment card fraud, account takeover fraud, and true name fraud – that fall under the legal term identity theft to better understand how criminal behavior patterns, risks for consumers and lenders, and mitigation strategies vary depending upon the sort of data stolen, the type of account compromised, and the opportunity for financial gain. Three areas key to developing effective solutions that, in the view of the author, would benefit from further definitional delineations are identified: measuring the success (or failure) of efforts to fight this crime, educating consumers about the risks and responses to this crime, and coordinating mitigation strategies across stakeholders and geographies.*

* Payment Cards Center, Federal Reserve Bank of Philadelphia, Ten Independence Mall, Philadelphia, PA 19106. E-mail: julia.cheney@phil.frb.org. The views expressed here are not necessarily those of this Reserve Bank or of the Federal Reserve System.

FEDERAL RESERVE BANK OF PHILADELPHIA

Ten Independence Mall, Philadelphia, PA 19106-1574 • (215) 574-7220 • www.philadelphiafed.org/pcc

Introduction

The Payment Cards Center (PCC) of the Federal Reserve Bank of Philadelphia studies issues in consumer payments that affect the financial services industry. An area of current focus is identity theft because, ultimately, these criminals are targeting financial services providers and, particularly, payment card providers. Further motivating the Center's course of study is this crime's potential to undermine consumer confidence in the industry's ability to deliver safe and secure financial products and services.[1]

Conducting this research makes it apparent that a critical issue in any discussion about identity theft lies in defining what we mean by that term. A legal definition was set forth in the Identity Theft and Assumption Deterrence Act of 1998. In this act, the term "identity theft" applies to the range of illegal activities that leverage a piece of personal information – defined in the act as a "means of identification" – to perpetrate a crime.[2] On this basis, many financial frauds are considered a form of identity theft crime because they generally rely on the compromise of personal data. For example, a credit card number is a "means of identification," per the act's definition, and therefore, identity theft is committed when a card number is stolen and used to make fraudulent purchases. This definition has been adopted in practice by law enforcement agencies and federal regulators.

However, the financial services industry tends to classify the fraudulent use of stolen card numbers as payment card fraud rather than identity theft. Furthermore, industry representatives argue that the range of criminal activity stemming from the compromise of personal data (i.e.,

[1] To examine identity theft from a variety of stakeholder perspectives and to explore coordinated solutions, the Payment Cards Center, in conjunction with the Gartner Fellows Program, hosted an identity theft forum in early 2004. See the PCC conference summary "Identity Theft: Where Do We Go From Here?," April 2004 (http://www.philadelphiafed.org/pcc/conferences/IdentityTheft_042004.pdf). Participants included representatives from the financial services and retail merchant industries, Internet service and technology providers, and regulatory and law enforcement agencies. This conference was motivated by an earlier PCC workshop on the topic led by Avivah Litan, vice president and research director of financial services at Gartner, Inc. See the PCC discussion paper "Identity Theft: A Pernicious and Costly Fraud," December 2003 (http://www.philadelphiafed.org/pcc/discussion/IdentityTheft_122003.pdf).

[2] For additional detail, the Identity Theft and Assumption Deterrence Act of 1998 can be found on the Federal Trade Commission's web site at www.ftc.gov/os/statutes/itada/itadact.htm.

identity theft) results in dissimilar forms of financial fraud, each exhibiting distinct attributes and a variety of consequences for victims and lenders. In addition, these factors are fundamental considerations when stakeholders are developing strategies to mitigate the effects of these crimes. To optimize strategies to combat identity theft, the industry wants more nuanced definitions as determined by the specific form of fraud and by the process used to identify and respond to its losses and its customers'.

The enactment of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) "raised the bar" on the definition debate. Now, besides using the definition of identity theft to trigger penalties in the criminal code, the FACT Act applies the definition to consumer rights and protections that assist in preventing identity theft and, in the case of victimization, in remedying its effects.[3] In essence, the definition of identity theft, and in particular how expansive this definition is in the FACT Act, determines the circumstances under which consumers and victims have access to the protections afforded in the act. The Federal Trade Commission (FTC) was charged with reviewing the FACT Act's definition of identity theft in light of its use in this legislation.

The FTC, in its Notice of Proposed Rulemaking and Request for Public Comment, proposed that the definition should be "sufficiently broad to cover all bona fide victims and conduct, but should be tailored to prevent individuals who are not identity theft victims from using the Act for unscrupulous purposes such as clearing negative, but legitimate, information from their credit records."[4] Following a comment period, on October 29, 2004, the FTC published its final ruling, making the FACT Act's definition of identity theft consistent with that already in place in the criminal code (see Exhibit 1). By confirming the expansive definition, the

[3] For additional detail on the identity theft provisions included in H.R. 2622 The Fair and Accurate Credit Transactions Act of 2003, see the Federal Trade Commission's web site at http://www.ftc.gov/opa/2004/06/factaidt.htm.

[4] Related Identity Theft Definitions, Duration of Active Duty Alerts, and Appropriate Proof of Identity under the Fair Credit Reporting Act, 69 FR 23370 (proposed April 28, 2004) (to be codified at 16 CFR, parts 603, 613, and 614), p. 6.

FTC has given all identity theft victims access to FACT Act rights and remedies in cases of fraud stemming from the compromise of personal data (per the "means of identification" definition),[5] including, for example, those the industry and others would characterize as payment card fraud.

Nevertheless, debate continues to center on one question: Does applying the broad definition of identity theft dilute the effectiveness of solutions developed in response to distinct forms of identity theft crime? In other words, do definitions still matter when protecting consumers from identity theft?

To consider this question, this paper begins with an examination of several types of financial fraud that fall under the legal term of identity theft: fictitious identity fraud, payment card fraud, account takeover fraud, and true name fraud.[6] By comparing and contrasting these frauds, the stage is set for a discussion of how their unique characteristics can affect the determination and priority given to detection strategies, mitigation efforts, and victim responses.[7] In particular, several features of identity theft crime, including the sort of data stolen, the type of account compromised, and the opportunity for financial gain, are found to be key variations in the pattern of criminal behavior. In each case, this paper shows how the distinctive criminal behavior pattern has influenced responses to these crimes. Finally, to answer the question of whether definitions still matter, this paper presents several examples where broadly applying the term identity theft may hinder stakeholders' efforts to develop solutions effective in combating specific forms of financial fraud.

While identity theft affects other groups, such as retail merchants, this paper primarily examines the effects from the perspective of consumers and bank lenders. Further, the analysis

[5] Related Identity Theft Definitions, Duration of Active Duty Alerts, and Appropriate Proof of Identity under the Fair Credit Reporting Act, 69 FR 63922 (Final Rule effective date December 1, 2004) (codified at 16 CFR, parts 603, 613, and 614), p.12.

[6] Although there may be additional and newly emerging forms of financial fraud that fall under the legal term of identity theft, I chose to focus on these four types.

[7] It should be noted that other names may be used by various groups to describe similar criminal activity but the hope is that by assigning these fraud terms and describing the activity associated with each, this paper will help to set a definitional baseline for future discussions of identity theft solutions.

focuses on how payment cards and related financial accounts are compromised when thieves use them to commit identity theft. The four financial frauds discussed herein are listed in increasing order of their potential to result in financial losses for consumers.

Fictitious Identity Fraud

Fictitious identity fraud is a financial crime in which pieces of real data, from one or more consumers, are combined with made-up information to fabricate an identity that does not belong to any real person. In a majority of cases, a completely new credit record[8] is established and linked to the fabricated identity. Related fraudulent activity is captured as part of this "new" credit file rather than that of any real individual's credit record. As a result, typically there are no consumer-victims of this crime to report the identity theft.

The pattern begins with thieves' efforts to build a payment history associated with the fictitious identity. To do so, the criminal establishes one or a few credit accounts, usually with lower credit lines, and makes payments on these balances as required. The positive record of payment performance increases the potential to obtain additional credit and to qualify for larger loan amounts. For example, the thief may begin by acquiring a cell phone account, making timely payments on the account, and following up with applications for credit cards and consumer loans, such as automobile financing. The objective is to open as many credit accounts as possible with a variety of credit providers: cell phone companies, financial institutions, and credit card issuers, among others. Once several accounts have been created, wherever possible each credit line is fully used. At this point, the thief "busts out"[9] and disappears, leaving creditors with the financial loss.

---

[8] A consumer's "credit file" (i.e., "credit record," "record of credit") is a record of how a person has borrowed and repaid debts. Credit files are maintained by credit reporting agencies such as Experian, Equifax, and TransUnion. For more information see the PCC Discussion Paper "An Overview and History of Credit Card Reporting," Mark Furletti, Payment Cards Center, June 2002. (http://www.philadelphiafed.org/pcc/discussion/CreditReportingHistory_062002.pdf)

[9] "Bust out" refers to the situation where thieves use an entire available credit line, monetize that line, and disappear leaving the credit provider to absorb the loss associated with the unpaid loan. Bust out fraud can be perpetrated by identity thieves as well as consumers who want to avoid paying legitimate debts. For

The bust out and disappearance of the account holder complicate detecting fictitious identity fraud. From the lender's perspective, the evidence includes (1) the account has gone delinquent and (2) collection teams have been unable to contact the account holder. On one hand, the account could have been legitimate, but for one of several reasons, such as a change in employment status, the account holder has decided to not repay the loan and to avoid collection-related efforts. Alternatively, the account may have been opened using a fabricated identity, and therefore, the account holder's disappearance may be an incidence of fraud. In either case, the lender's inability to contact the account holder undermines efforts to determine which situation the lender is dealing with. This same uncertainty hinders efforts to quantify financial losses resulting directly from fictitious identity fraud, and generally, without a clear indication of fraud, related charge-offs will be characterized as loan losses. One firm that offers identity-theft-detection solutions, ID Analytics, suggests that this form of identity theft accounts for "88.3 percent of all identity fraud events and 73.8 percent of the total dollars lost by U.S. businesses."[10] While a number of observers have argued that these estimates are overstated little published information, other than that from ID Analytics, is available to quantify the total dollar losses or incidence of fictitious identity fraud.

Despite the lack of quantifiable data, several characteristics known to be part of the criminal pattern have driven the development of mitigation strategies. For example, the criminal objective to create new accounts using newly established credit files has focused lenders' attention on the application process and, more specifically, on applications from individuals with so-called "thin" credit files (i.e., files with limited payment histories). Lenders are employing a variety of measures, including the use of external databases, to further verify application data submitted by these types of loan applicants. For example, an applicant's phone and address

---

more information on activity associated with "bust out fraud," see the PCC Discussion Paper "Fraud Management in the Credit Card Industry," p. 12. (http://www.philadelphiafed.org/pcc/discussion/FraudManagement_042002.pdf)

[10] ID Analytics, Inc. "ID Analytics Announces New Data Analysis Findings; Synthetic Identity Fraud Poses New Challenges," February 9, 2005. (http://www.idanalytics.com/news_and_events/2005209.html)

information can be compared against a database of existing phone book records. If the data submitted by the applicant are inconsistent with those in the database, the application can be flagged as a possible instance of fictitious identity fraud and further steps can be taken to verify the applicant's identity.

Although in most of these types of criminal cases it is the credit provider, not the individual consumer, that suffers the financial loss, consumers can help protect themselves and prevent this kind of fraud by guarding personal information.[11]

Payment Card Fraud

Payment card fraud (payment fraud)[12] is committed when thieves steal payment cards or the account numbers (i.e., credit or debit card account numbers) of existing financial accounts and use them to purchase goods and services. Payment fraud thieves may use the physical plastic card to make in-person transactions or only the card account number, expiration date, name of the account holder, and, in some cases, the card verification number to make transactions on the Internet and in other card-not-present environments. In either case, the fraudulent activity is generally restricted to a single account and to one or a few fraudulent transactions before it is detected and the compromised accounts are closed by the payment card issuer. At that point, a new account is opened for the consumer, and compromised payment cards are reissued with different account numbers. A crucial aspect of this criminal pattern is that control of the compromised account remains with the valid card holder and is not assumed by the thief. Therefore, the legitimate card holder continues to receive billing statements and marketing

[11] The Federal Reserve Bank of Philadelphia has published several brochures for consumers describing the steps consumers should take to protect their personal information and the steps to take if they do become victims. See http://www.philadelphiafed.org/pcc/consumer/index.html to access "Protecting Yourself Against Identity Theft" and "Preventing Payment Card Fraud: Dos and Don'ts."

[12] Payment fraud is a transactional-based fraud and is referred to by some constituencies as "transaction fraud." The discussion of payment fraud focuses on fraud committed using a payment card (i.e., credit or debit card) and does not extend to check fraud, which may be considered a variation of payment or transaction fraud. Check fraud deals with the manipulation of checks for financial gain.

information associated with the account. As a result, consumers are in a position to detect payment fraud by reviewing mailed statements monthly or online statements more frequently.

Payment fraud has been a fixture in the payment card industry since the industry's inception, and over the years, technology and consumer protection regulations have been used to address the problem. The payment card industry has been very successful in employing sophisticated detection software to flag unusual account activity. In some cases, such flags will even result in a call to the card holder to confirm purchasing behavior. Such technology has contributed to a declining trend in credit card fraud: Currently, in the U.S., fraud involving general purpose credit cards averages less than 0.06 percent of sales (see Exhibit 2). As further illustration, in 2004 total dollar losses from fraud were $788.3 million across credit card issuers operating on the Visa, MasterCard, American Express, and Discover networks, down from $882.5 million in fraud losses in 2003.[13] In the online environment, merchants are also employing a variety of fraud-detection tools that have resulted in a decreasing trend in the percentage of revenue lost due to payment fraud, decreasing from 3.6 percent in 2000 to 1.8 percent in 2004.[14]

In addition to technology solutions, federal law limits consumer liability for payment fraud, although protections vary depending on whether the fraud is credit card- or debit card-based. For example, fraudulent use of lost or stolen credit card information is limited to $50 per card, although, in most cases, card issuers waive this fee. For debit cards, liability protection depends on whether the plastic card itself is stolen and used fraudulently. If it is, a time element is added to the protection: Generally, if the theft of the card is reported within two business days of the customer learning of its theft, consumer liability is limited to $50. After two business days and within 60 days of the customer's receipt of the billing statement containing the fraudulent activity, consumer liability is limited to $500; after that, there is no legal liability limit. Alternatively, when thieves steal just the account number and use it either on its own or to

[13] *The Nilson Report*, Number 830, March 2005, pp. 1, 8.
[14] CyberSource Corporation, *6th Annual Online Fraud Report: Online Payment Fraud Trends and Merchants' Response – 2005 Edition*, p. 4.

produce a counterfeit plastic card, customers have zero liability for 60 days from receipt of the statement in which the fraudulent activity is reported and unlimited liability thereafter. Many institutions offer consumer protections greater than those required by law. [15]

Since payment fraud compromises existing financial accounts, efforts to detect and to mitigate it have focused on quickly identifying unusual transactions and putting in place practices to either confirm the validity of the purchase or deactivate the card. Another differentiating factor of this crime is that several market participants have the ability to detect the fraud: consumers who are actively monitoring their account activity, financial institutions that are employing technology solutions, or merchants who are helping to authenticate customers' identity. These efforts in combination with the legislated liability protections mean that consumers face relatively little financial risk from this form of identity theft.

Account Takeover Fraud

Account takeover fraud establishes control over an existing financial account – either a deposit or credit account – without the authority of the legitimate account holder. [16] To take over an account, thieves acquire consumers' information; many times an account number, Social Security number, and account access codes (i.e., personal identification number [PIN] or password) are sufficient to impersonate the valid account holder. Unlike payment fraud, where the fraudulent behavior is generally limited to a few transactions, account takeover fraud is more intrusive: The thieves attempt to steal the entire balance in a consumer's demand deposit account or to access the full credit line associated with a consumer's credit account.

[15] For more detail on consumer protections related to credit and debit cards, see the PCC Discussion Paper by Mark Furletti and Stephen Smith, "The Laws, Regulations, and Industry Practices That Protect Consumers Who Use Electronic Payment Systems: Credit and Debit Cards," January 2005 (http://www.philadelphiafed.org/pcc/ConsumerProtectionPaper_CreditandDebitCard.pdf).

[16] Account takeover has also been characterized as the "hijacking" of financial accounts. A recent report by the FDIC, "*Putting an End to Account-Hijacking Identity Theft*," presents the FDIC's findings on unauthorized access to financial institution accounts and how the financial industry and its regulators can mitigate these risks. See http://www.fdic.gov/consumers/consumer/idtheftstudy/.

Whether the compromised account is deposit- or credit-based has implications for the pattern of criminal behavior. With deposit accounts, identity thieves use stolen personal data to access victims' accounts and to initiate either fund withdrawals or balance transfers to alternative accounts under the thief's control. The objective is to deplete the available balance as quickly as possible before the fraud is discovered. When credit accounts are targeted, the criminal's objective is to fully use the available credit line and then bust out. One mechanism thieves use to delay detection of credit card takeover fraud is to request a change of address to redirect mailings of account information from the victim's address to the thief's. Once the address has been changed, the thief will often request an additional or replacement card be sent to the new address. These actions extend the time available to commit fraud and increase the thief's options for doing so.

Criminal patterns in account takeover are continuing to evolve as more consumers manage their financial accounts over the Internet. As an illustration, in a recent report by the Pew Internet & American Life Project, 53 million people, or one-quarter of all adults, were estimated to use online banking, a 47 percent increase over the number of Americans using online banking in 2002.[17] As this trend continues, personal account data and access codes are more widely communicated electronically between account holders and their banks. Motivated by these trends, thieves are increasingly acquiring technical sophistication in designing schemes to compromise account data stored on personal computers and transmitted electronically. Once the data are compromised, the anonymous nature of the Internet positions identity thieves to impersonate their victims and to direct account actions.

Online fraud schemes used by thieves to steal personal information are many and continually evolving. One example is phishing. This scheme involves broadly distributed e-mails that trick consumers into providing account and password information. These e-mails are made to

[17] *Online Banking 2005: A Pew Internet Project Data Memo*, Susannah Fox, 2/9/05. Pew Internet & American Life Project.

look as if they are being sent from and are linking to legitimate banking sites.[18] If these attempts are successful, phishing provides criminals with account numbers and related passwords: the keys to accessing victims' financial accounts. In 2004, global fraud losses for phishing attacks alone – just one method used to commit account takeover fraud – have been estimated in industry reports to be in the range of $100 million to $400 million.[19] However, available data to confirm these estimates are limited. Similarly, finding a data source to estimate total losses from the broader category of account takeover fraud is difficult.

Another method thieves use to collect the information necessary for account takeover is keystroke-logging software or other forms of spyware or malicious code. Keystroke-logging software can be hidden in an e-mail attachment that when clicked on, secretly downloads the code to the consumer's personal computer. When the consumer visits his banking site, the code captures the victim's keystrokes (i.e., password and account data) and sends them to a web site operated by the identity thief. With this information the identity thief is able to gain access to and transfer balances from the victim's financial accounts. In many cases, unless the victim has sophisticated firewall protection, the data are stolen without any indication to the valid account holder that such a compromise has occurred.

Understanding the criminal pattern of account takeovers has helped stakeholders, and particularly financial services providers, to isolate vulnerabilities exploited by identity thieves. Various stakeholder groups have pointed out the need for better ways to authenticate consumers' identities when providing access to financial accounts or authorizing purchases. Several

---

[18] For more information on phishing, see Frederick W. Stakelbeck, Jr., "Phishing: A Growing Threat to Financial Institutions and E-Commerce," Federal Reserve Bank of Philadelphia, *SRC Insights*, Fourth Quarter 2004 (http://www.philadelphiafed.org/src/srcinsights/srcinsights/q4si7_04.html).

[19] The reports referenced include those published by Financial Insights and TowerGroup. Financial Insights' report titled "Fraudsters Go Phishing in a Million Dollar Hole of Opportunity" estimates that "U.S. and international financial institutions stand to lose up to $400 million in fraud losses resulting from phishing incidents occurring in 2004" (http://www.financial-insights.com/FI/getdoc.jsp?containerId=pr2004_07_14_191436). In the press release announcing TowerGroup's report titled "A Phish Tale? Moving From Hype to Reality," co-author Beth Robertson was quoted as stating that "direct fraud losses attributable to phishing are expected to total just $137.1 million globally in 2004." (http://www.towergroup.com/research/content/news_view.jsp?newsId=147)

technology solutions are being considered as ways to improve customer authentication, including two-factor authentication techniques and biometrics, but no universal agreement has been reached or standard determined.[20]

When takeover fraud involves deposit accounts, banks are increasingly imposing, or allowing consumers to impose, limits on the daily amounts that can be transferred out of a demand deposit account in order to reduce thieves' ability to quickly clean out an account.[21] In addition, the FACT Act has established rules around the change of address process to limit its usefulness as a means to delay recognition of identity theft. With payment fraud consumer efforts focus primarily on monitoring account activity, but the criminal pattern in account takeover fraud is more complex and calls for additional preventive actions by consumers. In addition to monitoring transactional activity, these actions include confirming receipt of monthly account statements and related materials, instituting safe e-mail practices,[22] and securing personal computer systems. [23] These measures will help to limit thieves' ability to delay detection by requesting a "change of address" and to steal account information using methods such as phishing and keystroke logging.

Ultimately, consumers are generally protected from liability arising from account takeover fraud because federal regulation limits consumer liability related to the fraudulent or unauthorized use of lost or stolen credit and debit cards, including unauthorized electronic account withdrawals that don't involve a card (for example, ACH transfers initiated online). [24] Unlike payment card fraud, account takeover can affect victims' financial accounts more

---

[20] For more information describing customer authentication methods, see "The Use of Technology to Mitigate Account-Hijacking Identity Theft" in the FDIC report *Putting an End to Account-Hijacking Identity Theft*. (http://www.fdic.gov/consumers/consumer/idtheftstudy/technology.html#)

[21] Bob Sullivan, "Online bank fraud concerns consumers; Account holder rights vary based on situation," MSNBC, December 14, 2004.

[22] Safe e-mail practices include a) never submitting account information in response to an e-mail request, no matter who the sender appears to be, b) never opening attachments from unknown users, and c) when in doubt, calling the sender (organization) to confirm the validity of requests made via e-mail.

[23] Personal computer security includes timely installation of software patches released by providers and installation and updating firewall and virus protection software.

[24] In addition to Furletti and Smith, see the Electronic Fund Transfers Act and its implementing regulation, Regulation E. (http://www.federalreserve.gov/regulations/#e)

severely. A well-executed account takeover fraud may give the thief sufficient time to max out the victim's available credit line or deplete the balance in her demand deposit account. The related financial losses for lenders are also greater because the fraudulent activity is not limited to one or a few transactions, but rather the entire account is often fully compromised.

Account takeover fraud is set apart from fictitious identity fraud and payment fraud by its criminal objective: Account takeover thieves aim to control the existing financial accounts of real consumers. In comparison, payment fraud targets existing accounts, but generally it is limited to one or a few fraudulent transactions and does not result in the valid account holder losing control of the account. Fictitious identity fraud focuses on the creation of new credit accounts, rather than the compromise of existing accounts, and generally its victims are the credit providers, not consumers.

True Name Fraud

To this point in the discussion of identity theft, consumers have been in a position to detect fraudulent activity by monitoring existing accounts and their associated activity. Additionally, consumers are reasonably well protected by legislation.[25] True name fraud has the potential to cause greater financial and other harm to victims because it results in the creation of new credit accounts in the name of the consumer and without his or her knowledge.

True name fraud is the wholesale assumption of another person's identity in an effort to gain access to new credit. In this case, identity thieves steal personal information – such as name, address, and Social Security number – that allows them to use the victim's credit record when applying for new loans. As such, these identity thieves create access to new credit facilities, unbeknownst to the real consumer, which is an important distinction from payment card fraud

[25] The Truth in Lending Act, enacted in 1974, and its implementing regulation, Regulation Z, limit consumer liability for unauthorized use of an account holder's credit card. The Electronic Fund Transfer Act, enacted in 1978, and its implementing regulation, Regulation E, limit consumer liability in cases of unauthorized use of an account holder's debit card and unauthorized electronic fund transfers from an account.

and account takeover fraud, where the criminal intent is to compromise consumers' existing financial accounts.

As part of the criminal pattern, the identity thief will submit contact information for the fraudulent accounts that are not, and have never been, associated with the real consumer. Therefore, the victim never receives communications, such as statements, that would indicate the existence of these accounts and the incidence of fraud. Often, true name identity theft involves creating multiple credit accounts in the name of the victim, and the thief fully draws on them before busting out. This is similar to the criminal pattern in fictitious identity fraud except, in this case, a real consumer is victimized. Unless true name fraud is detected early, negative payment data related to these fraudulent accounts are reported to the national credit agencies and become part of the victim's credit record. As a result, this form of identity theft incurs not only direct financial losses for its victims but also other damaging effects, such as a deterioration in credit scores, higher interest rates, and an inability to access new loans (e.g., a mortgage.)[26]

Spurred by the potentially damaging effects of true name fraud and to help stakeholders better understand the scope of identity theft, the FTC released the "Identity Theft Survey Report" in September 2003.[27] This report estimated that financial losses associated with the creation of new accounts were $32.9 billion in business losses and $3.8 billion in consumer losses over the previous year. Further, this type of identity theft accounted for roughly one-third of the total number of identity theft victims, broadly defined, but two-thirds of the total financial costs. In addition, victims of new account identity theft took longer to discover the fraud than those experiencing fraud related to existing financial accounts and spent more time – 60 hours as compared to 15 hours – to resolve related problems.

Detecting true name fraud by either credit providers or consumers is complicated by two key factors: (1) the focus on creating new credit accounts rather than compromising existing

[26] As with most identity theft, other stakeholders, including financial institutions, retail merchants, and other service providers, also suffer financial losses from true name fraud.
[27] To view the full report, visit http://www.ftc.gov/os/2003/09/synovatereport.pdf.

accounts and (2) no obvious indication to victims that new credit accounts have been created using their stolen personal information. Obviously, detection strategies focused on monitoring existing account activity are futile. For issuers, detection efforts require focusing on identity verification and screening during the credit application process. Alternatively, consumers must have a means to verify that accounts opened in their name and included in their credit file are legitimate. Otherwise, consumers are likely to become aware of their victimization only after they have been denied credit or received calls from collections agencies or creditors. In either case, because the account was opened by an impersonator, the victim has generally faced a complicated and time-consuming process to close these accounts and to restore their credit standing. In particular, many times victims have had to prove that indeed they were the legitimate consumer and that the identified accounts were fraudulent, i.e., not opened by the victim, before such negative data were removed from the victim's credit record.

Partly in response to the findings in the FTC report and to assist victims in addressing the problems associated with true name fraud, Congress included in the FACT Act [28] provisions that grant important new protections, rights, and remediation tools for victims of identity theft. A key element of these provisions has been to help victims of true name fraud detect this crime and contain its effects. This legislation grants consumers the right to obtain a free copy of their credit report, annually, from each national credit reporting agency, to place a fraud alert on their credit file, and to block trade lines contained in their credit record stemming from identity theft. By having access to credit report files, consumers can verify that all accounts included in their report are legitimate and, if not, they can place a fraud alert immediately on their credit file to limit further compromises. Additionally, after completing other steps such as filing a police report, identity theft victims can block trade lines on their credit report that are the result of identity theft. These tools enable identity theft victims to limit true name fraud's effect on their credit scores

[28] For more information on the FACT Act and its identity theft provisions, see FTC testimony on Identity Theft and Social Security Numbers, June 15, 2004, before the Subcommittee on Social Security of the House Committee on Ways and Means, pp. 5-9. http://www.ftc.gov/os/testimony/040615idtheftssntest.pdf.

and on their ability to qualify for future loans.[29] In this sense, the FACT Act's identity theft provisions may be seen as an important source of consumer protection for true name fraud victims in much the same way that earlier legislation protects victims of payment card fraud and account takeover fraud.

Do Definitions Still Matter?

Clearly, these four forms of identity theft exhibit unique characteristics that influence the risks and outcomes for victims and lenders as well as the priority given to counter-measures. At the same time, in each of these cases, industry stakeholders are developing mitigation strategies that are in part driven by the characteristics of the fraud but that also align with the regulatory requirements set forth in the FACT Act. As a result, the debate about whether definitions still matter continues to center on the question: Does applying the broad definition of identity theft dilute the effectiveness of solutions developed in response to distinct forms of identity theft crime?

This analysis suggests that definitions do matter and that a more refined set of generally accepted definitions would lead to improvements in at least three critical areas in the search for solutions to identity theft crime. These include measuring the success (or failure) of efforts to fight this crime, educating consumers about the risks and responses to this crime, and coordinating mitigation strategies across stakeholders and geographies.

Despite the legal definition of identity theft, there are important distinctions among these crimes, including their potential to result in financial losses for consumer-victims and bank

[29] Consumers can get help from other sources as well. For instance, the financial services sector has developed a broad array of initiatives aimed at helping true name fraud victims navigate the processes necessary to report the crime, correct credit report errors due to identity theft, and close affected accounts. In addition, this sector has collaborated on efforts to assist victims, educate consumers, and share data with law enforcement. An example of financial services industry collaboration is the Identity Theft Assistance Center (ITAC). Sponsored by the Financial Services Roundtable's technology arm, BITS, and its member institutions, ITAC is a centralized source launched to help victims notify and register fraudulent accounts with financial firms at which identity theft may have occurred. Moreover, ITAC is working to provide incidence tracking data to law enforcement agencies and to the FTC.

lenders. Applying the broad definition of identity theft makes it difficult to quantify financial costs, incidence rates, and criminal arrest rates associated with the sub-categories of identity theft. This data gap affects financial institutions when they evaluate the effectiveness of counter-measures targeting specific financial frauds. It affects law enforcement when assessing whether these types of financial frauds are increasing or decreasing and the implications of such trends. Also, it affects policymakers attempting to identify appropriate legislative or regulatory remedies to these various crimes. Perhaps most important, the data gap affects consumers' ability to accurately assess their relative risk of becoming a victim or, if they are victims, their potential financial and other losses. As a result, consumers may alter behaviors to protect against the most harmful form of identity theft, true name fraud, rather than matching their precautions to specific threats. For example, applying an overly broad definition may result in unintended consequences such as creating unwarranted fears among consumers about using electronic payments and commerce.

Providing a deeper and more nuanced view of the financial losses, incidence trends, and other available metrics associated with these crimes assists all stakeholders in accurately assessing their risk and in making decisions related to their allocation of resources. To date, there is wide variation in the extent to which categories of identity theft crime are tracked. For example, little information is available to assess the extent of fictitious identity fraud, but credit card payment fraud has been closely monitored and reported for many years. More detailed research to quantify incidence and loss trends would help provide answers to critical questions about how we are doing in addressing specific types of financial crimes related to identity theft and whether we have dedicated enough resources to fighting these frauds.

Another area on which many stakeholders are focusing attention is consumer education. The Federal Trade Commission has been in the fore of these efforts and has published several

pamphlets and other materials to assist consumers who are victimized by identity theft.[30] Additionally, other regulatory agencies, industry groups, and law enforcement agencies are stressing consumer education in the fight against identity theft. However, the lack of agreement about the definition creates confusion for consumers as they search for the best ways to manage their exposure and to limit losses related to these financial crimes.

More specificity in defining various types of identity theft crime would facilitate the development of educational materials that address the different strategies required for victims to respond to different criminal threats. For example, victims of payment card fraud should immediately report the unauthorized use to their card issuer. In the case of true name fraud, victims should first place a fraud alert on their credit file, obtain a copy of their credit report, file a police report, and contact issuers with whom fraudulent accounts have been opened. Furthermore, publications and web sites that explain which circumstances require identity theft victims to file a police report would assist in appropriately managing law enforcement resources and related costs. [31] Ultimately, by providing consumers with an understanding of the various types of identity theft, educational materials would better assist consumers not only in accurately assessing their risk of victimization but also in effectively and cost efficiently responding to these crimes.

Finally, the growing use of the Internet as a global platform for consumers to manage financial accounts has transformed identity theft into an international crime, one that can be perpetrated remotely and anonymously with thieves and victims in different regions of the world. In turn, law enforcement, the financial services industry, and regulators need to coordinate efforts to combat identity theft not only within their own countries but also internationally. Therefore,

---

[30] "Take Charge: Fighting Back Against Identity Theft," Federal Trade Commission. (http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm). Also, see the Federal Trade Commission's web site for consumer information on identity theft (http://www.consumer.gov/idtheft/).

[31] For example, victims of payment card fraud do not need to file a police report in order to access the liability protections granted under the Truth in Lending Act or the Electronic Fund Transfer Act. However, victims of true name fraud must file a police report in order to access their rights under the FACT Act.

definitions applied to identity theft must be communicated to the relevant parties and differences must be recognized across cultural and geographical boundaries in order to successfully track these crimes, determine criminal patterns, and fight identity theft fraud on a global scale.

Conclusion

To consider the question of whether definitions still matter, this paper has examined four financial frauds that fall under the legal definition of identity theft: fictitious identity fraud, payment card fraud, account takeover fraud, and true name fraud. These frauds were described in some detail, highlighting distinct characteristics of the criminal patterns and the mitigation strategies for each (see Exhibit 3).

This paper advances the argument that definitions still matter in several areas key to the development of identity theft solutions. It does not call for changes to enacted legislation nor to the legal definition of the term. Rather it asks all stakeholders, particularly the regulatory community, to consider the need for more descriptive definitions in support of the legal term in order to help speed progress on developing solutions and, ultimately, to aid efforts to protect consumers from the effects of each form of financial fraud that is legally identity theft crime.

Exhibit 1: Identity Theft Definition – A Comparison: Criminal Code vis-à-vis Consumer Protection Regulation

Definition in the criminal code: Identity Theft and Assumption Deterrence Act of 1998

This act made it a crime of identity theft when someone "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable State or local law." In the act "means of identification" was defined as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any

> (A) name, Social Security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
> (B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
> (C) unique electronic identification number, address, or routing code; or
> (D) telecommunication identifying information or access device (as defined in section 1029(e).

The term "access device" is defined in 18 U.S.C. 1029(e) to mean "any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)."

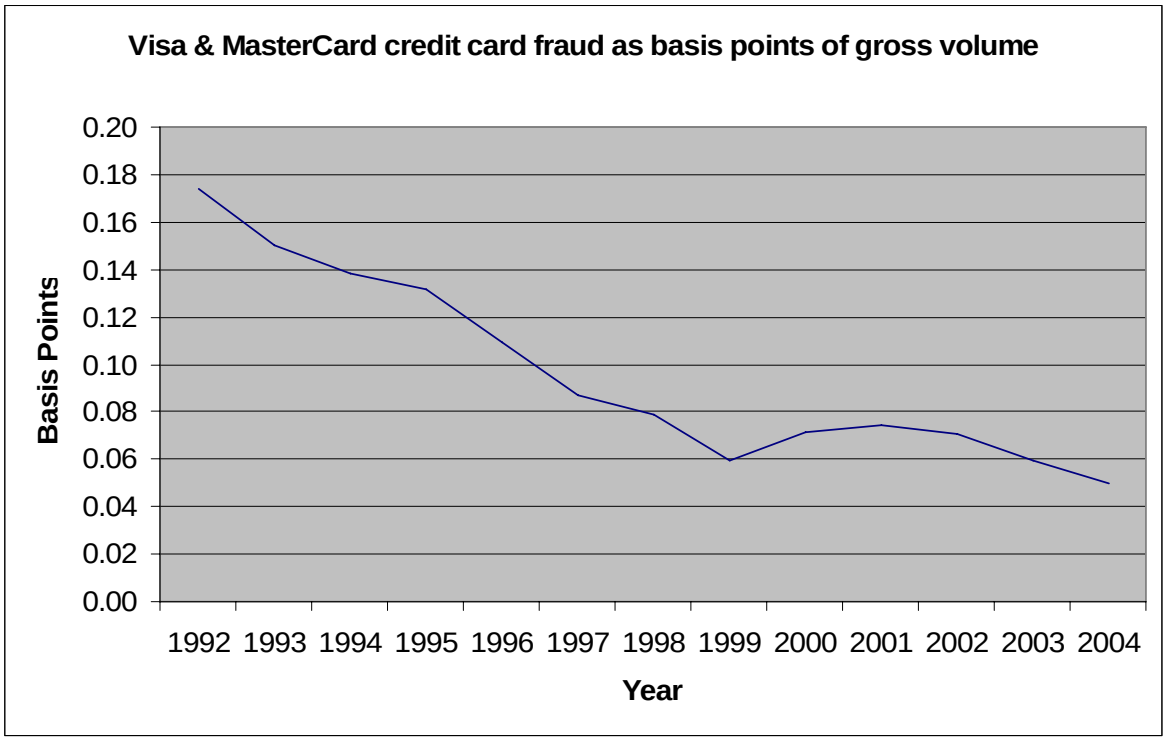
Definition in consumer protection regulation: Fair and Accurate Credit Transactions Act of 2003

The Federal Trade Commission's final rule defined identity theft as:

(a) A fraud committed or attempted using the identifying information of another person without authority.
(b) The term "identifying information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any
    1) name, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
    2) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
    3) unique electronic identification number, address, or routing code; or
    4) Telecommunications identifying information or access device (as defined in 18 U.S.C 1029(e)).[32]

[32] Federal Trade Commission, 16 CFR Parts 603, 613, and 614 RIN 3084-AA94 Related Identity Theft Definitions, Duration of Active Duty Alerts, and Appropriate Proof of Identity Under the Fair Credit Reporting Act.

Exhibit 2: Visa & MasterCard Trends in Credit Card Fraud



Data Source: *The Nilson Report*, various issues.

Exhibit 3: A Comparison of Identity Theft Frauds

	Fictitious Identity Fraud	Payment Card Fraud	Account Takeover Fraud	True Name Fraud
Brief Definition	Pieces of real data, from one or more consumers, are combined with made-up information to fabricate an identity that does not belong to any real person. In most cases a completely new credit record is established and linked to the fabricated identity.	Stolen payment cards or the account numbers (i.e., credit or debit card account numbers) of existing financial accounts are used to purchase goods and services.	Control over an existing financial account is established without authority of the legitimate account holder. Thieves attempt to steal the entire balance in a consumer's demand deposit account or to access the full credit line associated with a consumer's credit account.	The wholesale assumption of another person's identity in an effort to gain access to new credit. Thieves steal personal information - such as name, address, and Social Security number -- that allows them to use the victim's credit record when applying for new loans.
Consumer Victim?	No	Yes	Yes	Yes
Account Compromised	New Credit Account	Existing Financial Account	Existing Financial Account	New Credit Account
Loss Estimates	Unknown	Credit card: $788.3M, 2004 Debit card: unknown	Total losses are unknown. Phishing estimates range from $100M - $400M.	FTC report estimates $32.9B in business losses and $3.8B in consumer losses.
How Can Consumers Help With Detection?	Guard personal data (to protect against all identity theft)	Monitor account activity > Monthly statements > Frequent online review	- Monitor account activity > Monthly statements > Frequent online review - Confirm receipt of money statements/acct. information - Maintain personal computer security - Use safe e-mail practices	Review credit reports
Immediate Consumer Responses	N/A	Notification to bank/card issuer of unauthorized use	Notification to bank/card issuer of unauthorized use	- Obtain copy of credit report - Place a fraud alert on credit file - File a police report - Notify issuers where fraud may have occurred
Issuer/Bank Mitigation Strategy	Focus on improving application screening process to identify inconsistent data and flagging these applications for further review.	Focus on monitoring customers' existing account activity.	Focus on monitoring customers' existing account activity and controlling access to consumers' financial accounts, e.g., customer authentication.	Focus on improving application screening for new accounts.